DEPLOYMENT GUIDE

# SSL Insight Certificate Installation Guide

## Table of Contents

### Disclaimer

This document does not create any express or implied warranty about A10 Networks or about its products or services, including but not limited to fitness for a particular use and noninfringement. A10 Networks has made reasonable efforts to verify that the information contained herein is accurate, but A10 Networks assumes no responsibility for its use. All information is provided "as-is." The product specifications and features described in this publication are based on the latest information available; however, specifications are subject to change without notice, and certain features may not be available upon initial product release. Contact A10 Networks for current information regarding its products or services. A10 Networks' products and services are subject to A10 Networks' standard terms and conditions.

## Introduction

A prerequisite for configuring A10 Networks Thunder® SSL Insight® (SSLi®) solution is generating a Certificate Authority (CA) certificate with a known private key which will be used to re-sign the original server certificate when the client initiates an SSL session to the server. This CA certificate must be trusted by the internal users, or it must be signed by an own/local root CA trusted by the users. Otherwise, internal users will see an SSL "untrusted root" error whenever they try to connect to an SSL-enabled website.

This guide assumes a scenario where you have a local root CA and it issues (or signs) an intermediate CA certificate for an SSL Insight deployment. Also, the root CA certificate needs to be distributed and installed as Trusted Authority onto the internal client machines. This guide includes the following contents of SSL certificate installation:

- Generating CA certificates for SSL Insight
- Importing a CA certificate and certificate chain onto the A10 Thunder SSLi device
- Installing a certificate in Microsoft Windows 7 for Microsoft Internet Explorer
- Installing a certificate in Google Chrome
- Installing a certificate in Mozilla Firefox

## Generating CA Certificates for SSL Insight

The SSL Insight feature relies on a CA certificate and key pair to decrypt traffic between clients and any external SSL servers that are not controlled by the same organization. When an internal user initiated the SSL communication with an external server, the A10 Thunder SSLi device intercepts the server certificate from the original server, modifies the certificate and then re-signs it using the CA certificate. The forged server certificate is then sent to the internal user as a server certificate of the original server.

In the following example, a Linux server with an OpenSSL package installed is used as a root Certificate Authority (CA), and creates the root CA certificate. For SSL Insight use, Thunder SSLi generates a CSR to create an intermediate CA certificate which must be signed by root CA. Once generated, both intermediate CA certificate and CA certificate chain need to be imported onto the Thunder SSLi device.

1. Create a root pair (certificate and key) on root CA/Linux Server.

   This step shows how to create a root CA certificate and private key using OpenSSL on a Linux server. You can skip this if you already have own root CA.

   ```
   # openssl genrsa -aes256 -out private/ca.key.pem 4096
   # openssl req -config openssl.cnf -key private/ca.key.pem -new -x509 -days
   7300 -sha256 -extensions v3_ca -out certs/ca.cert.pem
   Enter pass phrase for private/ca.key.pem:
   You are about to be asked to enter information that will be incorporated
   into your certificate request.
   What you are about to enter is what is called a Distinguished Name or a
   DN.
   There are quite a few fields but you can leave some blank
   For some fields there will be a default value,
   If you enter ‘.’, the field will be left blank.
   -----
   Country Name (2 letter code) [AU]:US
   State or Province Name [Some-State]:CA
   Locality Name []:
   Organization Name [Internet Widgits Pty Ltd]:A10 Lab
   Organizational Unit Name []:SSLi Test
   Common Name []:A10 Lab Root CA
   Email Address []:
   ```

   ***Note***: *X509 v3_ca extension includes the following. For more details, refer https://jamielinux.com/docs/openssl-certificate-authority/index.html*

```
basicConstraints = critical, CA:true
keyUsage = critical, cRLSign, keyCertSign
subjectKeyIdentifier=hash
```

2. Create a private key and a CSR on the Thunder SSLi device.

   This is an example of how to create a private key and generate a CSR for intermediate CA certificate on the Thunder SSLi device.

   ```
   ThunderSSLi(config)# pki create csr ssli-ca.key use-mgmt-port scp://<IP
   address of your Linux server>/folder_path/ssli-ca.csr
   User name []?
   Password []?
   input key bits(1024,2048,4096) default 1024:2048
   input Common Name, 1~64:A10 SSLi Demo CA
   input Division, 0~31:
   input Organization, 0~63:A10 Lab
   input Locality, 0~31:
   input State or Province, 0~31:CA
   input Country, 2 characters:US
   input email address, 0~64:
   ```

   ***Note**: You can also create an intermediate pair (key and CA certificate) on your root CA without using CSR with Thunder SSLi.*

3. Sign the CSR and create an intermediate CA certificate on root CA/Linux server.

   This is an example of signing the CSR and creation of an intermediate CA certificate on root CA.

   ```
   # openssl ca -config openssl.cnf -extensions v3_intermediate_ca -days 3650
   -notext -md sha256 -in csr/ssli-ca.csr -out newcerts/ssli-ca.cert.pem
   Using configuration from openssl.cnf
   Enter pass phrase for /root/ca/private/ca.key.pem:
   Check that the request matches the signature
   Signature ok
   Certificate Details:
           Serial Number: 4099 (0x1003)
           Validity
               Not Before: May 26 01:41:10 2016 GMT
               Not After : May 24 01:41:10 2026 GMT
           Subject:
               countryName               = US
               stateOrProvinceName       = CA
               organizationName          = A10 Lab
               commonName                = A10 SSLi Demo CA
           X509v3 extensions:
               X509v3 Subject Key Identifier:

   75:78:9B:F1:A1:20:BD:7C:B3:5D:C6:2E:B3:AF:34:77:4D:5C:6C:2B
               X509v3 Authority Key Identifier:

   keyid:07:28:03:E3:B8:D1:EB:4F:17:05:FC:27:3C:D2:A8:74:F9:F2:C4:E9

               X509v3 Basic Constraints: critical
                   CA:TRUE, pathlen:0
               X509v3 Key Usage: critical
                   Digital Signature, Certificate Sign, CRL Sign
   Certificate is to be certified until May 24 01:41:10 2026 GMT (3650 days)
   Sign the certificate? [y/n]:y
   ```

```
 1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

4. (Optional) Create the certificate chain.

   This is an optional step required only if your intermediate CA certificate for SSLi is signed by another trusted intermediate CA instead of a root CA. In this case, a CA certificate chain is required to complete the chain of trust when an application verifies the server certificate signed by the intermediate CA which is not directly signed by root CA. The CA certificate chain can be created by concatenating the intermediate CA certificates from the one for SSL Insight up to the one signed by the root CA. If the intermediate CA certificate for SSLi is signed by the root CA, you don't need to create a certificate chain, as the user should have the root CA certificate as a trusted authority.

   For example, If the ssli-ca.cert.pem is signed by an intermediate CA (int-ca.cert.pem) which is signed by root CA, the certificate chain should include two certificate except root CA (ca.cert.pem).

```
root CA (ca.cert.pem)
         |
         +------ Int. CA (int-ca.cert.pem)
                         |
                         +------ SSLi CA cert (ssli-ca.cert.pem)
# cat newcerts/ssli-ca.cert.pem certs/int-ca.cert.pem > newcerts/ssli-ca-
chain.cert.pem
```

   ***Note**: You can also include root CA into the certificate chain but is not necessary.*

## Importing a CA Certificate and Certificate Chain onto the A10 Thunder SSLi Device

Once the intermediate CA and certificate chain are ready, you can import both as a certificate type onto the Thunder SSLi device for SSLi use. Since CSR is used, the private key (ssli-ca.key) is already on the Thunder SSLi.

```
#import cert ssli-ca.cert.pem certificate-type pem use-mgmt-port scp://<IP
address>/path/ssli-ca.cert.pem
#import cert ssli-ca-chain.cert.pem certificate-type pem use-mgmt-port
scp://<IP address>/path/ssli-ca-chain.cert.pem
```

***Note**: If you created a private key along with the intermediate CA certificate, you can export them in PKCS12 format on CA root server, and import it as pfx type on the Thunder SSLi.*

Once certificates are imported, you can configure them as forward-proxy certificate in the client-ssl template. Please note that the intermediate CA "ssli-ca.cert.pem" is used for both the CA certificate and certificate chain as it's signed by the root CA.

```
ThunderSSLi (config)#slb template client-ssl cSSLi
ThunderSSLi (config-client ssl)#forward-proxy-ca-cert ssli-ca.cert.pem
ThunderSSLi (config-client ssl)#chain-cert ssli-ca.cert.pem
ThunderSSLi (config-client ssl)#forward-proxy-ca-key ssli-ca.key
ThunderSSLi (config-client ssl)#forward-proxy-enable
ThunderSSLi (config-client ssl)#sh context
!
ThunderSSLi configuration: 172 bytes
!
slb template client-ssl cSSLi
  chain-cert ssli-ca.cert.pem
  forward-proxy-ca-cert ssli-ca.cert.pem
  forward-proxy-ca-key ssli-ca.key
  forward-proxy-enable
!
```

***Note**: In case a certificate chain is required, use the following command instead:*

```
ThunderSSLi (config-client ssl)#chain-cert ssli-ca-chain.cert.pem
```

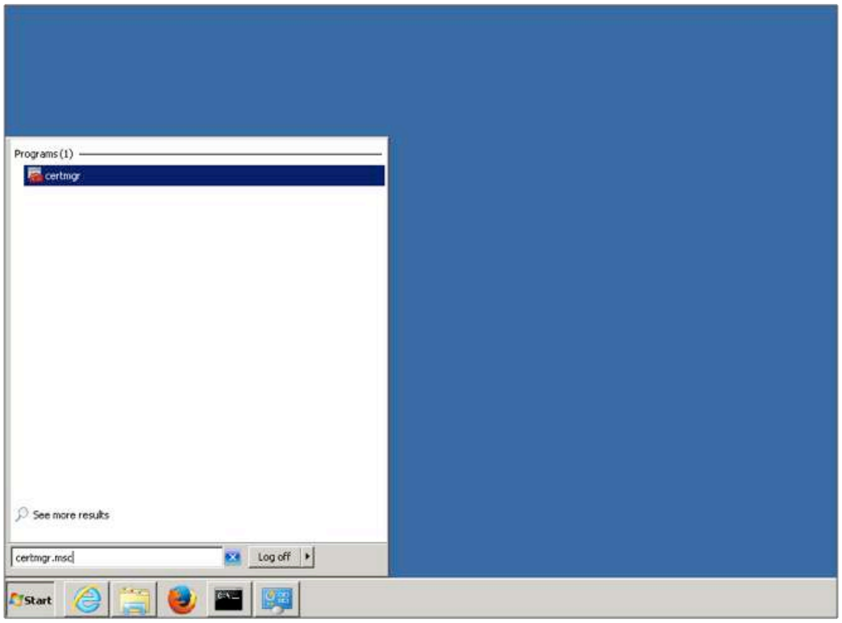
The root CA certificate must be imported as a Trust Authority onto the client machines. This can be done manually or by using an automated service such as Microsoft Group Policy Manager.

***Note**: Further details for Group Policy Manager can be found at: http://technet.microsoft.com/en-us/library/cc772491.aspx*

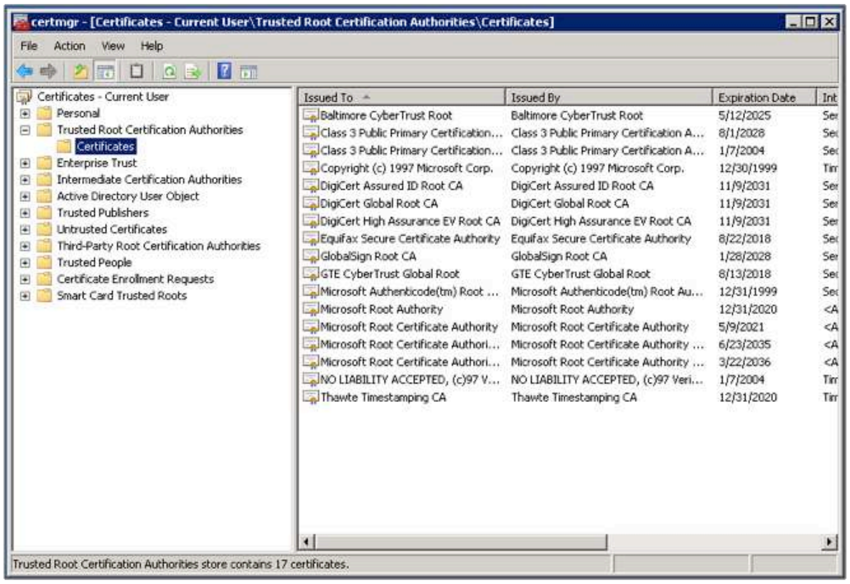
## Installing a Certificate in Microsoft Windows 7 for Internet Explorer

The following will guide you through the steps required for importing the root CA certificate into your Windows 7 computer. You must be logged on as an administrator to perform these steps and the root CA certificate should have been imported onto your computer already.

1. Open Certificate Manager by clicking the Start button, typing **certmgr.msc** into the search box, and then pressing Enter. If you're prompted for an administrator password or confirmation, type the password or provide confirmation.



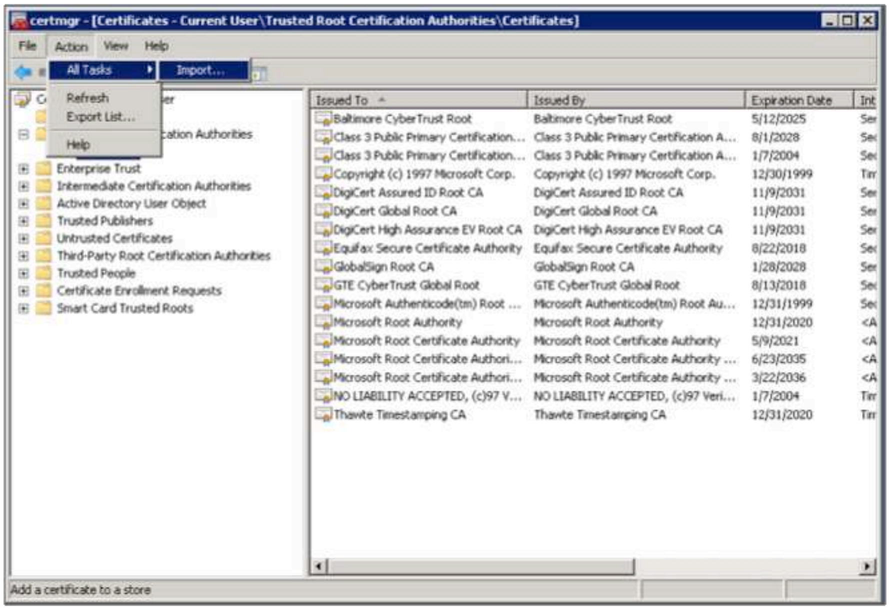
2. In **Certificate Manager**, select the folder that you want to import the certificate into. In this exercise, we have selected the folder: **Trusted Root Certification Authorities > Certificates**.


certmgr - [Certificates - Current User\Trusted Root Certification Authorities\Certificates]
File
Action
View
Help
Certificates - Current User
Personal
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Certificate Enrollment Requests
Smart Card Trusted Roots

| Issued To | Issued By | Expiration Date | Int |
|---|---|---|---|
| Baltimore CyberTrust Root | Baltimore CyberTrust Root | 5/12/2025 | Ser |
| Class 3 Public Primary Certification… | Class 3 Public Primary Certification A… | 8/1/2028 | Sec |
| Class 3 Public Primary Certification… | Class 3 Public Primary Certification A… | 1/7/2004 | Sec |
| Copyright (c) 1997 Microsoft Corp. | Copyright (c) 1997 Microsoft Corp. | 12/30/1999 | Tim |
| DigiCert Assured ID Root CA | DigiCert Assured ID Root CA | 11/9/2031 | Ser |
| DigiCert Global Root CA | DigiCert Global Root CA | 11/9/2031 | Ser |
| DigiCert High Assurance EV Root CA | DigiCert High Assurance EV Root CA | 11/9/2031 | Ser |
| Equifax Secure Certificate Authority | Equifax Secure Certificate Authority | 8/22/2018 | Sec |
| GlobalSign Root CA | GlobalSign Root CA | 1/28/2028 | Ser |
| GTE CyberTrust Global Root | GTE CyberTrust Global Root | 8/13/2018 | Sec |
| Microsoft Authenticode(tm) Root … | Microsoft Authenticode(tm) Root Au… | 12/31/1999 | Sec |
| Microsoft Root Authority | Microsoft Root Authority | 12/31/2020 | <A |
| Microsoft Root Certificate Authority | Microsoft Root Certificate Authority | 5/9/2021 | <A |
| Microsoft Root Certificate Authori… | Microsoft Root Certificate Authority … | 6/23/2035 | <A |
| Microsoft Root Certificate Authori… | Microsoft Root Certificate Authority … | 3/22/2036 | <A |
| NO LIABILITY ACCEPTED, (c)97 V… | NO LIABILITY ACCEPTED, (c)97 Veri… | 1/7/2004 | Tim |
| Thawte Timestamping CA | Thawte Timestamping CA | 12/31/2020 | Tim |

Trusted Root Certification Authorities store contains 17 certificates.

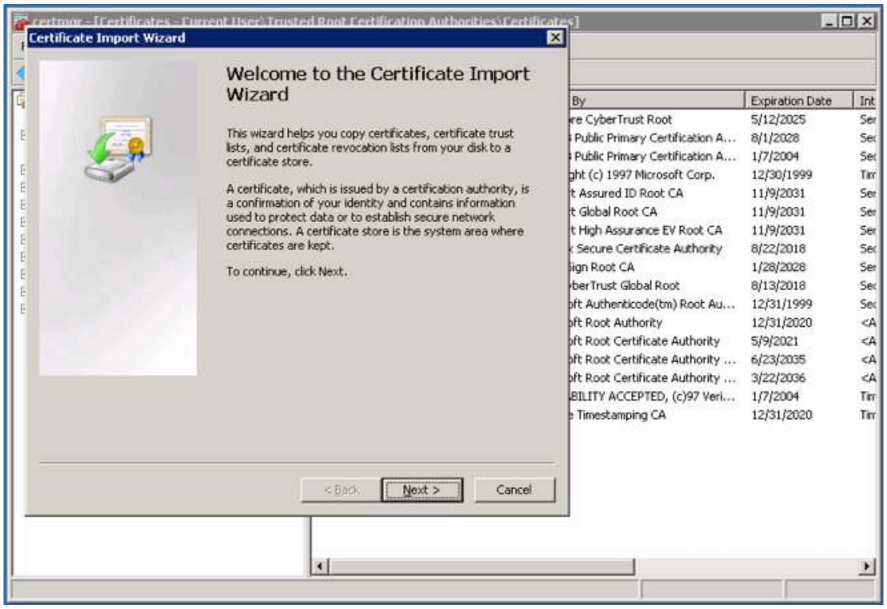
3. Click the **Action** menu, point to **All Tasks**, and then click **Import**.


certmgr - [Certificates - Current User\Trusted Root Certification Authorities\Certificates]
File
Action
View
Help
All Tasks
Import...
Refresh
Export List...
Help
ation Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Certificate Enrollment Requests
Smart Card Trusted Roots

| Issued To | Issued By | Expiration Date | Int |
|---|---|---|---|
| Baltimore CyberTrust Root | Baltimore CyberTrust Root | 5/12/2025 | Ser |
| Class 3 Public Primary Certification... | Class 3 Public Primary Certification A... | 8/1/2028 | Sec |
| Class 3 Public Primary Certification... | Class 3 Public Primary Certification A... | 1/7/2004 | Sec |
| Copyright (c) 1997 Microsoft Corp. | Copyright (c) 1997 Microsoft Corp. | 12/30/1999 | Tim |
| DigiCert Assured ID Root CA | DigiCert Assured ID Root CA | 11/9/2031 | Ser |
| DigiCert Global Root CA | DigiCert Global Root CA | 11/9/2031 | Ser |
| DigiCert High Assurance EV Root CA | DigiCert High Assurance EV Root CA | 11/9/2031 | Ser |
| Equifax Secure Certificate Authority | Equifax Secure Certificate Authority | 8/22/2018 | Sec |
| GlobalSign Root CA | GlobalSign Root CA | 1/28/2028 | Ser |
| GTE CyberTrust Global Root | GTE CyberTrust Global Root | 8/13/2018 | Sec |
| Microsoft Authenticode(tm) Root ... | Microsoft Authenticode(tm) Root Au... | 12/31/1999 | Sec |
| Microsoft Root Authority | Microsoft Root Authority | 12/31/2020 | <A |
| Microsoft Root Certificate Authority | Microsoft Root Certificate Authority | 5/9/2021 | <A |
| Microsoft Root Certificate Authori... | Microsoft Root Certificate Authority ... | 6/23/2035 | <A |
| Microsoft Root Certificate Authori... | Microsoft Root Certificate Authority ... | 3/22/2036 | <A |
| NO LIABILITY ACCEPTED, (c)97 V... | NO LIABILITY ACCEPTED, (c)97 Veri... | 1/7/2004 | Tim |
| Thawte Timestamping CA | Thawte Timestamping CA | 12/31/2020 | Tim |

Add a certificate to a store

4. In **Certificate Import Wizard**, click **Next** to proceed to the **File Import** page.


certmgr - [Certificates - Current User\Trusted Root Certification Authorities\Certificates]
Certificate Import Wizard
< Back
Next >
Cancel

Welcome to the Certificate Import Wizard

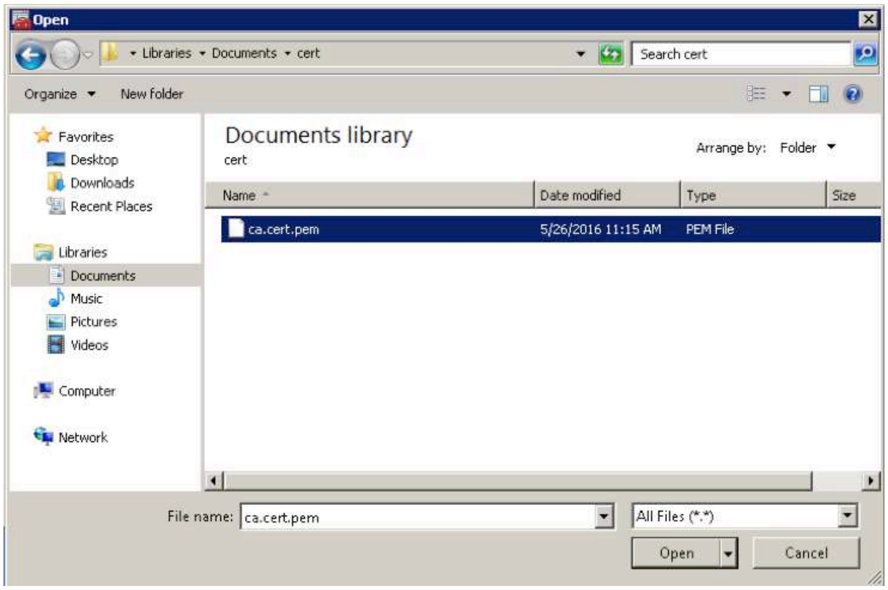
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

5. Select **Browse** to locate the certificate file that is to be imported.

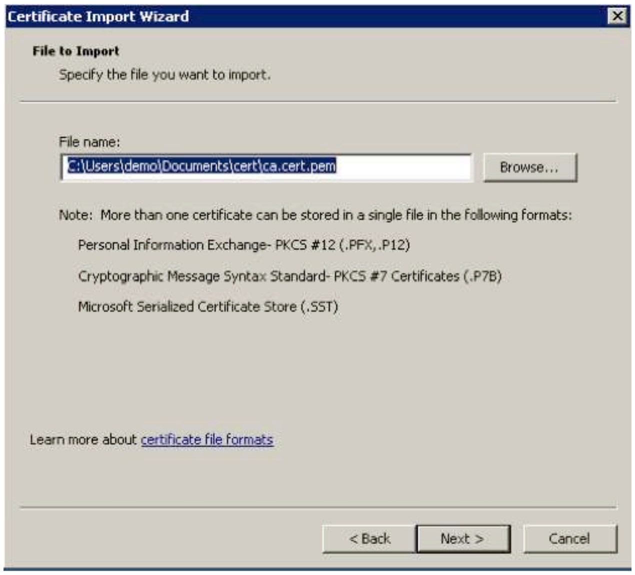
***Note**: the **Open** dialog box only displays X.509 certificates by default. If you want to import another type of certificate, select the certificate type you want to import in the **Open** dialog box and click **Open**.*



| Name | Date modified | Type | Size |
|---|---|---|---|
| ca.cert.pem | 5/26/2016 11:15 AM | PEM File | |

File name: ca.cert.pem

6. Click the **Next** button.



**File to Import**

Specify the file you want to import.

File name:
C:\Users\demo\Documents\cert\ca.cert.pem

Note: More than one certificate can be stored in a single file in the following formats:

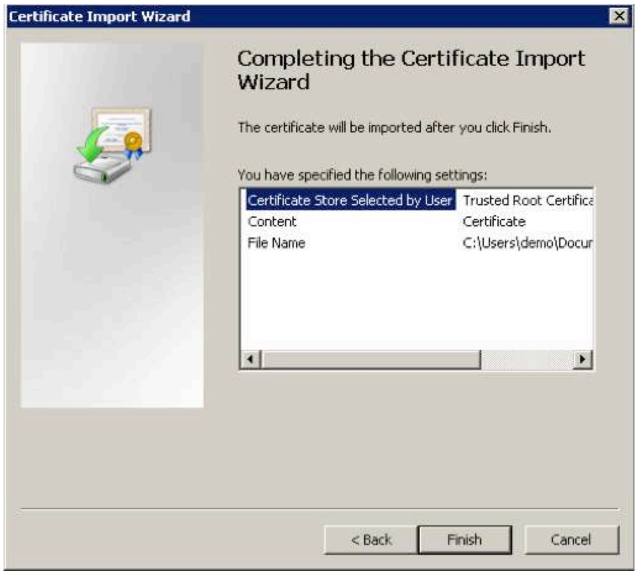
Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

7. Click the **Next** button.



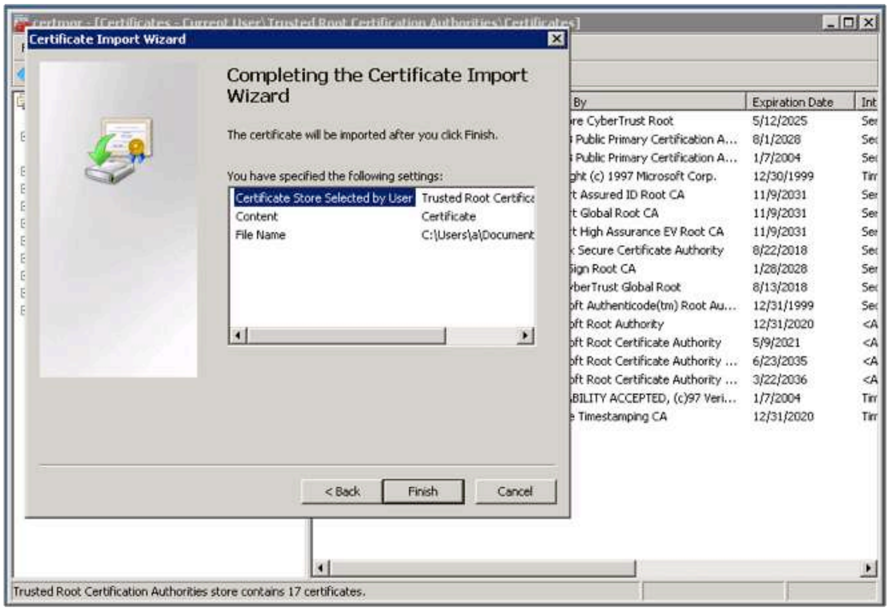
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

| | |
|---|---|
| Certificate Store Selected by User | Trusted Root Certifica |
| Content | Certificate |
| File Name | C:\Users\demo\Docur |

8. Confirm your selections and click **Finish**.



certmgr - [Certificates - Current User\Trusted Root Certification Authorities\Certificates]
Certificate Import Wizard
< Back
Finish
Cancel

Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

| | |
|---|---|
| Certificate Store Selected by User | Trusted Root Certifica |
| Content | Certificate |
| File Name | C:\Users\a\Document |

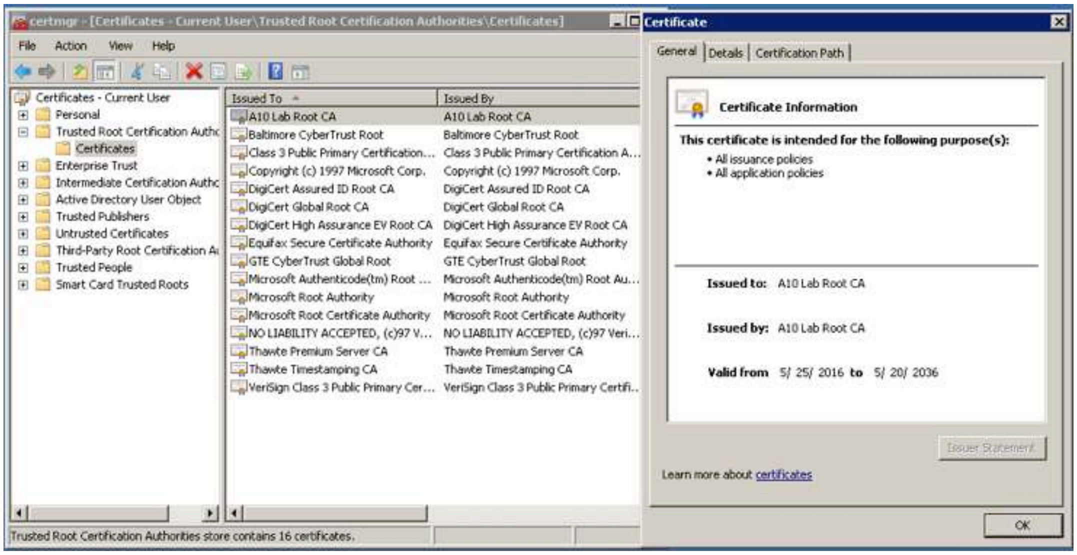
| By | Expiration Date | Int |
|---|---|---|
| re CyberTrust Root | 5/12/2025 | Ser |
| Public Primary Certification A... | 8/1/2028 | Sec |
| Public Primary Certification A... | 1/7/2004 | Sec |
| ght (c) 1997 Microsoft Corp. | 12/30/1999 | Tim |
| t Assured ID Root CA | 11/9/2031 | Ser |
| t Global Root CA | 11/9/2031 | Ser |
| t High Assurance EV Root CA | 11/9/2031 | Ser |
| Secure Certificate Authority | 8/22/2018 | Sec |
| ign Root CA | 1/28/2028 | Ser |
| berTrust Global Root | 8/13/2018 | Sec |
| ft Authenticode(tm) Root Au... | 12/31/1999 | Sec |
| ft Root Authority | 12/31/2020 | <A |
| ft Root Certificate Authority | 5/9/2021 | <A |
| ft Root Certificate Authority ... | 6/23/2035 | <A |
| ft Root Certificate Authority ... | 3/22/2036 | <A |
| BILITY ACCEPTED, (c)97 Veri... | 1/7/2004 | Tim |
| Timestamping CA | 12/31/2020 | Tim |

Trusted Root Certification Authorities store contains 17 certificates.

9. In the **Security Warning** popup, select **Yes**, since you made an informed decision to import this certificate.

10. If the import is successful, you will see a dialog box with the message "**The import was successful**."

11. You can see the newly installed CA certificate under the specified folder.



certmgr - [Certificates - Current User\Trusted Root Certification Authorities\Certificates]
File
Action
View
Help
Certificates - Current User
Personal
Trusted Root Certification Authc
Certificates
Enterprise Trust
Intermediate Certification Authc
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Au
Trusted People
Smart Card Trusted Roots
Certificate
General
Details
Certification Path
Issuer Statement
OK

| Issued To | Issued By |
|---|---|
| A10 Lab Root CA | A10 Lab Root CA |
| Baltimore CyberTrust Root | Baltimore CyberTrust Root |
| Class 3 Public Primary Certification… | Class 3 Public Primary Certification A… |
| Copyright (c) 1997 Microsoft Corp. | Copyright (c) 1997 Microsoft Corp. |
| DigiCert Assured ID Root CA | DigiCert Assured ID Root CA |
| DigiCert Global Root CA | DigiCert Global Root CA |
| DigiCert High Assurance EV Root CA | DigiCert High Assurance EV Root CA |
| Equifax Secure Certificate Authority | Equifax Secure Certificate Authority |
| GTE CyberTrust Global Root | GTE CyberTrust Global Root |
| Microsoft Authenticode(tm) Root … | Microsoft Authenticode(tm) Root Au… |
| Microsoft Root Authority | Microsoft Root Authority |
| Microsoft Root Certificate Authority | Microsoft Root Certificate Authority |
| NO LIABILITY ACCEPTED, (c)97 V… | NO LIABILITY ACCEPTED, (c)97 Veri… |
| Thawte Premium Server CA | Thawte Premium Server CA |
| Thawte Timestamping CA | Thawte Timestamping CA |
| VeriSign Class 3 Public Primary Cer… | VeriSign Class 3 Public Primary Certifi… |

Trusted Root Certification Authorities store contains 16 certificates.

Certificate Information

This certificate is intended for the following purpose(s):
- All issuance policies
- All application policies

Issued to: A10 Lab Root CA

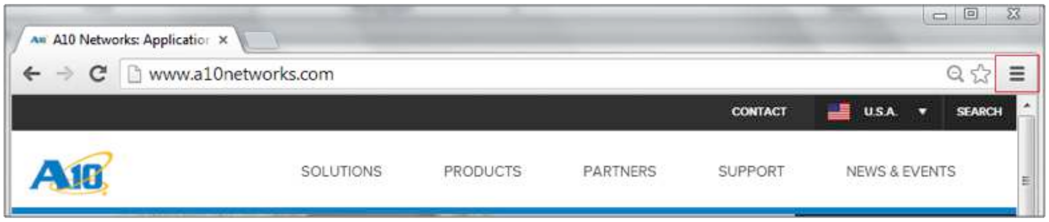
Issued by: A10 Lab Root CA

Valid from 5/ 25/ 2016 to 5/ 20/ 2036

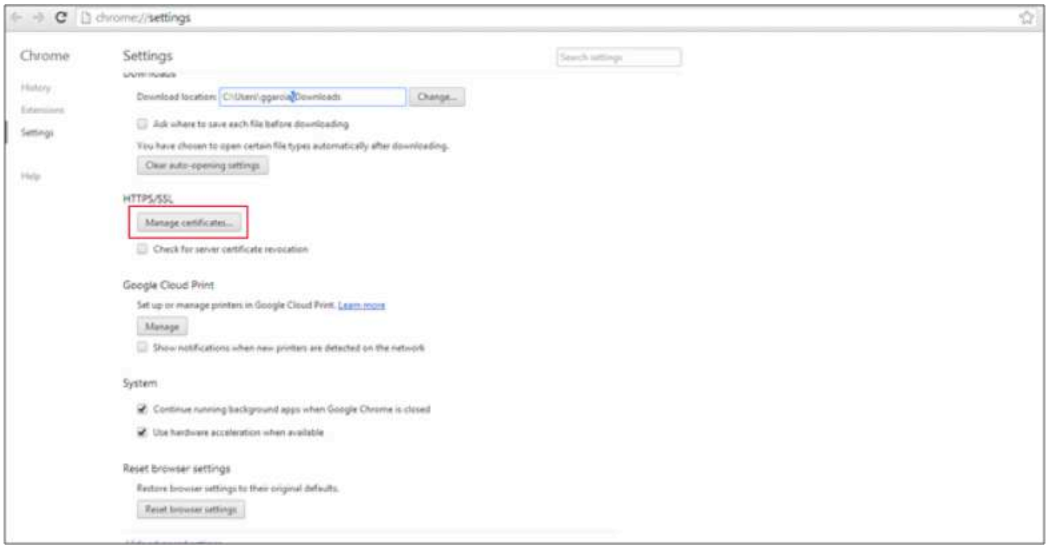
Learn more about certificates

## Installing a Certificate in Google Chrome

1. To install the CA certificate on Google Chrome, open the Chrome browser.
2. Click the "**Customize and Control Google Chrome**" option located on the right hand corner of the browser window.



3. Navigate to the **HTTPS/SSL** section of Chrome Settings and click the **Manage certificates** button.



Download location: C:\Users\ggarcia\Downloads Change...

☐ Ask where to save each file before downloading

You have chosen to open certain file types automatically after downloading.

Clear auto-opening settings

HTTPS/SSL

Manage certificates...

☐ Check for server certificate revocation

Google Cloud Print

Set up or manage printers in Google Cloud Print. Learn more

Manage

☐ Show notifications when new printers are detected on the network

System

☑ Continue running background apps when Google Chrome is closed

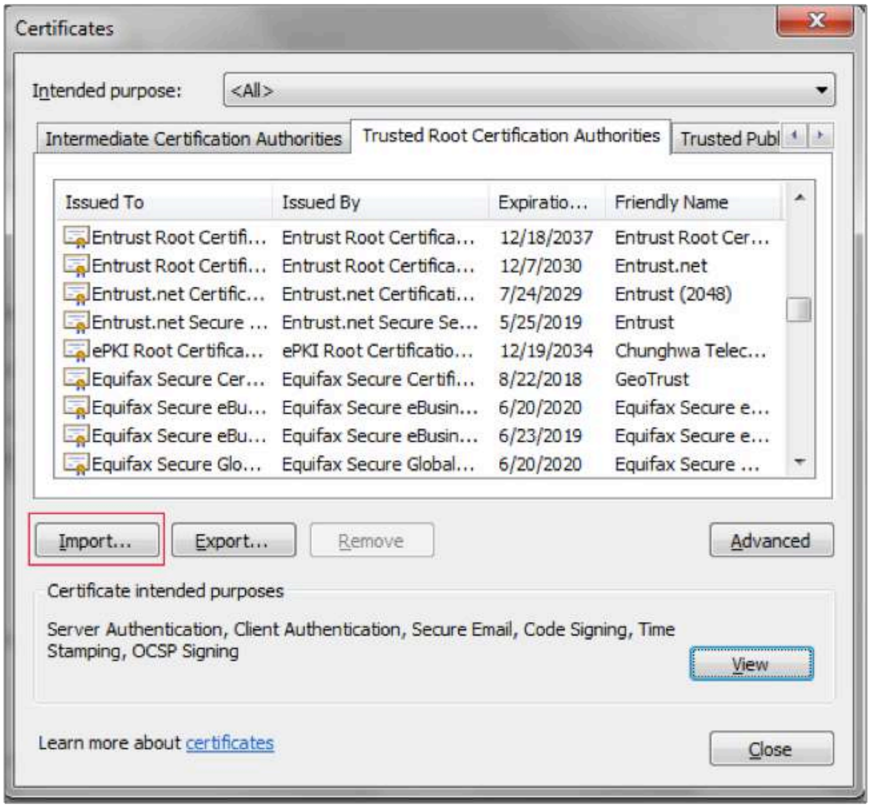
☑ Use hardware acceleration when available

Reset browser settings

Restore browser settings to their original defaults.

Reset browser settings

4. In the certificate folder on the **Trusted Root Certification Authorities** tab, click the **Import** button and a **Certificate Import Wizard** will appear.



Certificates

Intended purpose: <All>

Intermediate Certification Authorities
Trusted Root Certification Authorities
Trusted Publ

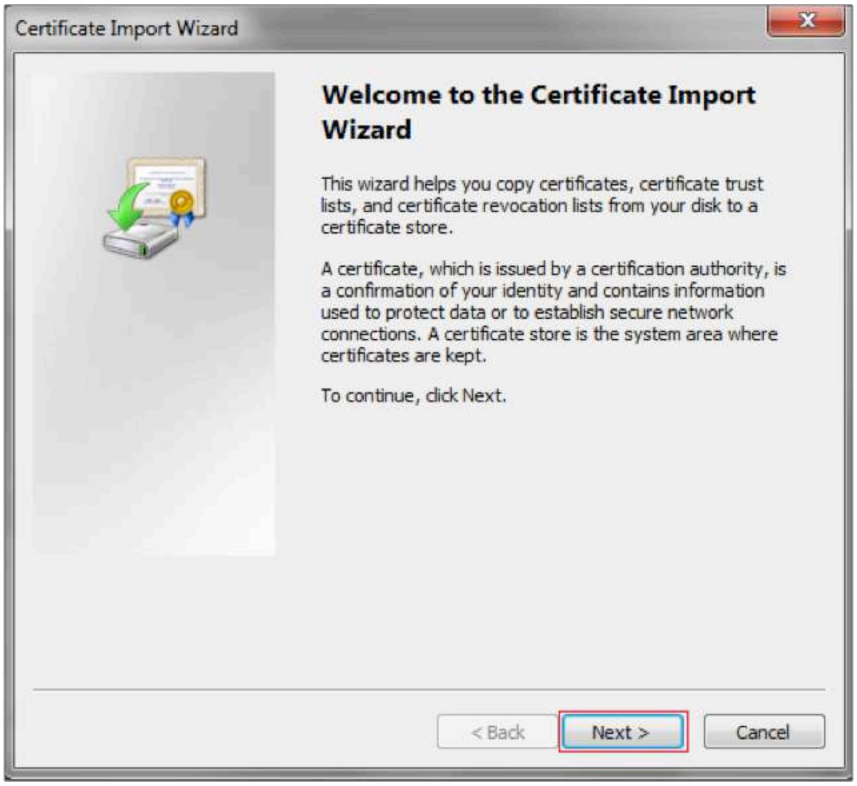
| Issued To | Issued By | Expiratio... | Friendly Name |
|---|---|---|---|
| Entrust Root Certifi... | Entrust Root Certifica... | 12/18/2037 | Entrust Root Cer... |
| Entrust Root Certifi... | Entrust Root Certifica... | 12/7/2030 | Entrust.net |
| Entrust.net Certific... | Entrust.net Certificati... | 7/24/2029 | Entrust (2048) |
| Entrust.net Secure ... | Entrust.net Secure Se... | 5/25/2019 | Entrust |
| ePKI Root Certifica... | ePKI Root Certificatio... | 12/19/2034 | Chunghwa Telec... |
| Equifax Secure Cer... | Equifax Secure Certifi... | 8/22/2018 | GeoTrust |
| Equifax Secure eBu... | Equifax Secure eBusin... | 6/20/2020 | Equifax Secure e... |
| Equifax Secure eBu... | Equifax Secure eBusin... | 6/23/2019 | Equifax Secure e... |
| Equifax Secure Glo... | Equifax Secure Global... | 6/20/2020 | Equifax Secure ... |

Certificate intended purposes

Server Authentication, Client Authentication, Secure Email, Code Signing, Time Stamping, OCSP Signing

Learn more about certificates

5. In the **Certificate Import Wizard**, click the **Next** button.



Certificate Import Wizard

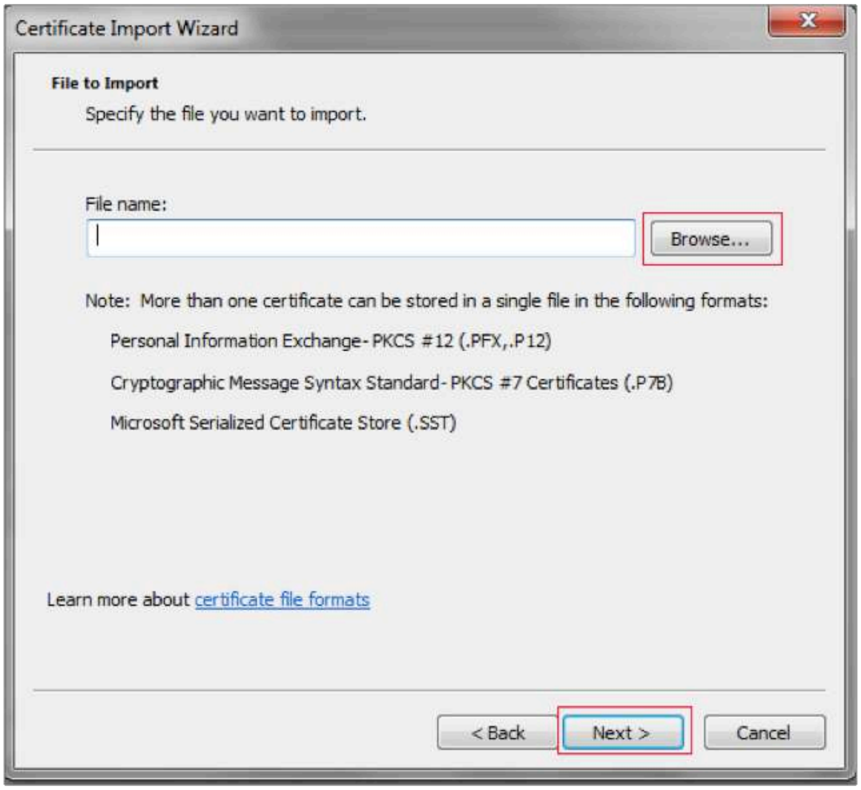
**Welcome to the Certificate Import Wizard**

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

6. Click the **Next** button to browse to the location of the CA certificate.



**File to Import**

Specify the file you want to import.

File name:

Note: More than one certificate can be stored in a single file in the following formats:

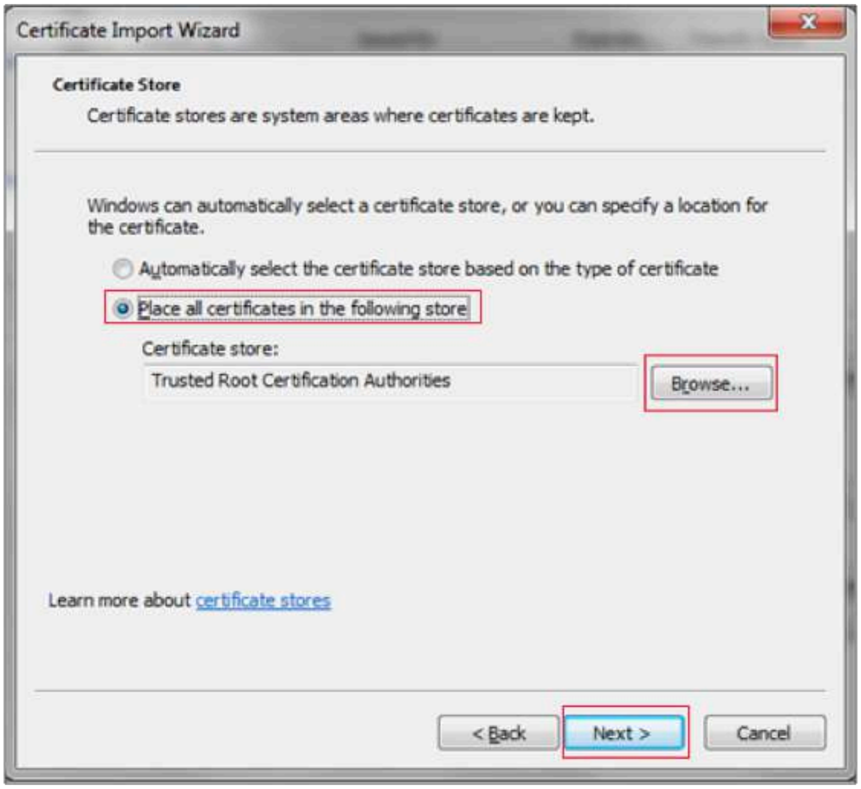
Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

7. Once the correct certificate has been located, click **Next** to install the certificate in the "Trusted Root Certificate Authorities" certificate store. Click **Next** and **Finish** and then click **OK**. You will see a Security Warning pop-up, select Yes, since you made an informed decision to import this certificate.



**Certificate Store**

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

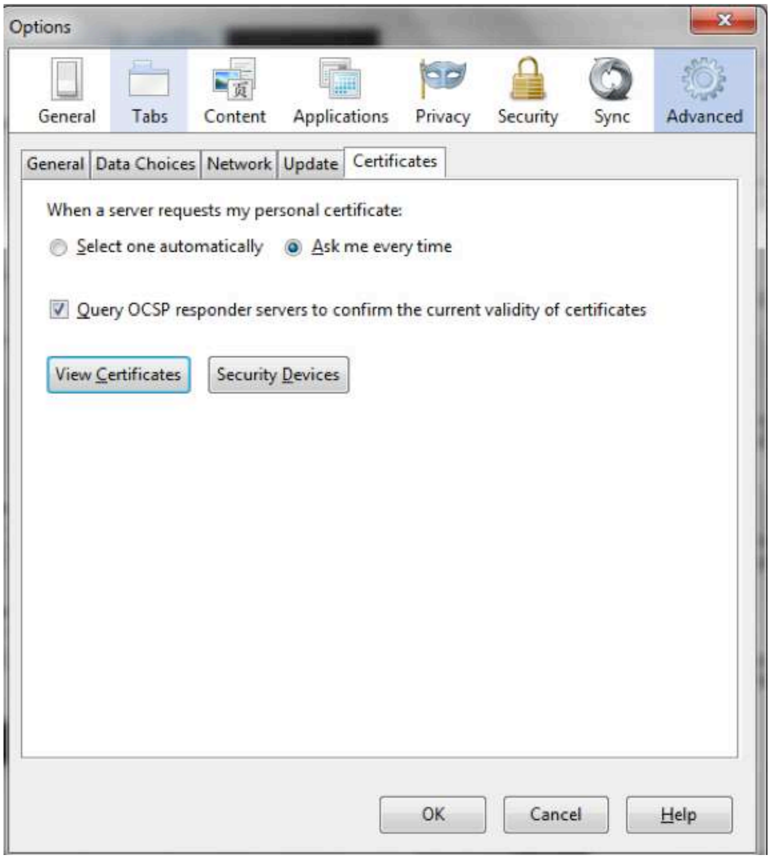
Trusted Root Certification Authorities

Learn more about certificate stores

## Installing a Certificate in Mozilla Firefox

Mozilla Firefox utilizes a certificate store and all root CA certificates are stored within the certificate store. In order for SSL Insight to perform properly, each client must download and install the SSL root certificate. Otherwise, Firefox will generate an error message warning clients about SSL error connection attempts.

1. To install a SSL root certificate in Firefox, launch the Firefox browser and open the **Options** window.

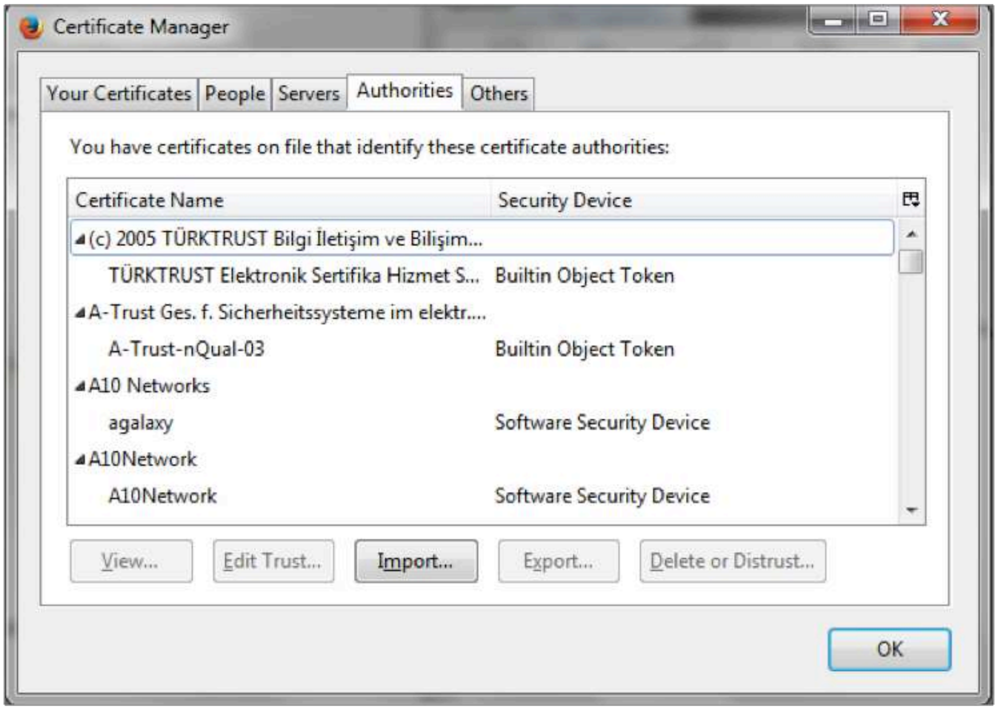


When a server requests my personal certificate:

○ Select one automatically ● Ask me every time

☑ Query OCSP responder servers to confirm the current validity of certificates

2. From the Options window, select the **Advanced** settings option and then click the **Certificate** tab. From the **Certificates** window, click the **View Certificates** button. Mozilla will display the **Certificate Manager** dialog.

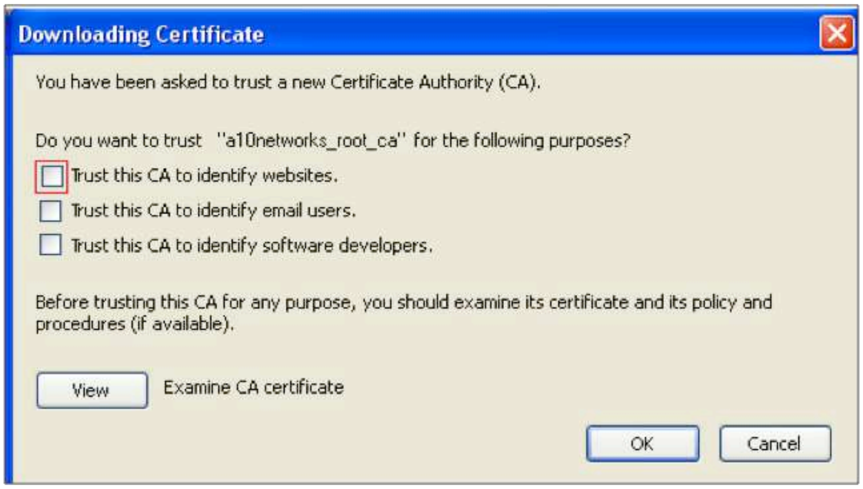


You have certificates on file that identify these certificate authorities:

| Certificate Name | Security Device |
|---|---|
| ◢(c) 2005 TÜRKTRUST Bilgi İletişim ve Bilişim... | |
| TÜRKTRUST Elektronik Sertifika Hizmet S... | Builtin Object Token |
| ◢A-Trust Ges. f. Sicherheitssysteme im elektr.... | |
| A-Trust-nQual-03 | Builtin Object Token |
| ◢A10 Networks | |
| agalaxy | Software Security Device |
| ◢A10Network | |
| A10Network | Software Security Device |

3. Click the **Import** button.

4. Navigate to where the certificate is located and click **Open**. A **Downloading Certificate** window will be displayed.



You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "a10networks_root_ca" for the following purposes?

☐ Trust this CA to identify websites.

☐ Trust this CA to identify email users.

☐ Trust this CA to identify software developers.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

Examine CA certificate

5. Select the **Trust this CA to identify websites** checkbox and click **OK**. Now, the certificate should be imported and the client machine can access HTTPS applications without receiving an error message.

## About A10 Networks

A10 Networks is a leader in application networking, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, California, and serves customers globally with offices worldwide. For more information, visit: **www.a10networks.com**

### Corporate Headquarters

**A10 Networks, Inc**
**3 West Plumeria Ave.**
**San Jose, CA 95134 USA**
**Tel: +1 408 325-8668**
**Fax: +1 408 325-8666**
**www.a10networks.com**

Part Number: A10-SB-16140-EN-03
Aug 2016

### Worldwide Offices

**North America**
sales@a10networks.com
**Europe**
emea_sales@a10networks.com
**South America**
latam_sales@a10networks.com
**Japan**
jinfo@a10networks.com
**China**
china_sales@a10networks.com
**Hong Kong**
hongkong@a10networks.com
**Taiwan**
taiwan@a10networks.com
**Korea**
korea@a10networks.com
**South Asia**
southasia@a10networks.com
**Australia/New Zealand**
anz_sales@a10networks.com

To discover how A10 Networks products will enhance, accelerate and secure your business, contact us at **a10networks.com/contact** or call to speak with an A10 sales representative.